

The Weight Hierarchies and Chain Condition of a Class of Codes from Varieties over Finite Fields

Xinwen Wu, Gui-Liang Feng, T. R. N. Rao*

July 16, 1996

Abstract

The generalized Hamming weights of linear codes were first introduced by Wei, which are fundamental parameters related to the minimal overlap structures of the subcodes and very useful in several fields. It was found that the chain condition of a linear code is convenient in studying the generalized Hamming weights of the product codes. In this paper we consider a class of codes defined over some varieties in projective spaces over finite fields, whose generalized Hamming weights can be determined by studying the orbits of subspaces of the projective spaces under the actions of classical groups over finite fields, i.e., the symplectic groups, the unitary groups and orthogonal groups. We gave the weight hierarchies and generalized weight spectra of the codes from Hermitian varieties and prove that the codes satisfy the chain condition.

Index Terms: weight hierarchy, chain condition, codes from varieties, classical groups

1 Introduction

The generalized Hamming weights of a linear code were introduced by V. K. Wei [1]. Let \mathbb{F}_q be a finite field, where q is a prime power. For any code D of block length n over \mathbb{F}_q , define the *support* $\chi(D)$ by

$$\chi(D) = \{i \mid c_i \neq 0 \text{ for some } (c_1, c_2, \dots, c_n) \in D\},$$

*Xinwen Wu, Gui-Liang Feng, T. R. N. Rao are with the Center for Advanced Computer Studies, University of Southwestern Louisiana, Lafayette, LA. 70504, USA. email: xw@swamp.cacs.usl.edu, glf@swamp.cacs.usl.edu and rao@swamp.cacs.usl.edu. This work was supported in part by the National Science Foundation under Grant NCR-9505619, Louisiana Education Quality Support Fund under Grant LEQSF-(1994-96)-RD-A-36, and NASA Project NAG-W-4013,

and the *support weight* $w_s(D)$ by

$$w_s(D) = |\chi(D)|.$$

Let C be a linear $[n, k]$ code over \mathbb{F}_q . For any r , where $1 \leq r \leq k$, the r -th *generalized Hamming weight* of C is defined as

$$d_r(C) = \min\{ w_s(D) \mid D \text{ is an } r\text{-dimensional subcode of } C \}.$$

Obviously, the minimum Hamming weight (minimum distance) of C is just $d_1(C)$. The *weight hierarchy* of C is then defined to be the set of generalized Hamming weights

$$\{d_1(C), d_2(C), \dots, d_k(C)\}.$$

The following properties of the generalized Hamming weights are known for a q -ary $[n, k]$ code C .

(1) (Monotonicity) $1 \leq d_1(C) < d_2(C) < \dots < d_k(C) \leq n$.

(2) (Duality) Let C^\perp be the dual code of C . Then

$$\{d_r(C^\perp) \mid 1 \leq r \leq n - k\} = \{1, 2, \dots, n\} \setminus \{n + 1 - d_r(C) \mid 1 \leq r \leq k\}.$$

Many applications of generalized Hamming weights are known. They are useful in cryptography [1][2], in trellis coding [3][4], and in truncating a linear block code [5], etc..

The support weight distribution for irreducible cyclic codes was introduced by Helleseth, Kløve, and Mykkeltveit [10]. The generalized Hamming weights are actually the minimum support weights.

We say that a linear $[n, k]$ code C satisfies the *chain condition*, if there exist r -dimensional subcode D_r of C for $1 \leq r \leq k$ such that

$$w_s(D_r) = d_r(C), \quad r = 1, 2, \dots, k.$$

and

$$D_1 \subset D_2 \subset \dots \subset D_k.$$

The following proposition can be found in [11],

Proposition 1 *If C satisfies the chain condition, so does its dual code C^\perp .*

In this paper we consider a class of codes defined over some varieties in projective spaces over finite fields, whose generalized Hamming weights can be determined by studying the orbits of subspaces of the projective spaces under the actions of classical groups over finite fields. We gave the weight hierarchies and generalized weight spectra of the codes from Hermitian varieties and prove that the codes satisfy the chain condition.

2 The codes from varieties and classical groups

Now let us consider the finite field \mathbb{F}_{q^2} with q^2 elements, where q is a power of prime. \mathbb{F}_{q^2} has an involutive automorphism

$$a \longmapsto \bar{a} = a^q.$$

The fixed field of this automorphism is \mathbb{F}_q .

Let $k = \nu + l$, where $\nu > 0$, $l \geq 0$. The set of points ${}^t(x_1, x_2, \dots, x_k)$ satisfying

$$x_1^{q+1} + x_2^{q+1} + \dots + x_\nu^{q+1} = 0$$

is a Hermitian variety in $PG(k-1, \mathbb{F}_{q^2})$, when $l = 0$, it is a nondegenerate Hermitian variety, and when $l > 0$, it is a degenerate Hermitian variety. We denote this Hermitian variety by $I_{(\nu, l)}$. Let $n = |I_{(\nu, l)}|$ be the number of points lying on $I_{(\nu, l)}$ in $PG(k-1, \mathbb{F}_{q^2})$. Then from [14], we have

$$\begin{aligned} n &= \frac{(q^\nu - (-1)^\nu)(q^{\nu-1} - (-1)^{\nu-1})}{q^2 - 1} q^{2l} + \frac{q^{2l} - 1}{q^2 - 1} \\ &= \frac{q^{2\nu+2l-1} + (-1)^{\nu-1} q^{\nu+2l-1} + (-1)^\nu q^{\nu+2l} - 1}{q^2 - 1}. \end{aligned} \quad (2)$$

For each point of $I_{(\nu, l)}$, choose a system of coordinates and regard it as a k -dimensional column vector. Arrange these n column vectors in any order into $k \times n$ matrix, denote it also by $I_{(\nu, l)}$. It can be proved that $I_{(\nu, l)}$ is of rank k . Hence $I_{(\nu, l)}$ can be regarded as a generator matrix of a q^2 -ary projective $[n, k]$ -code, which will be denoted by $C_{(\nu, l)}$. Obviously,

$$S_{C_{(\nu, l)}, I_{(\nu, l)}} = I_{(\nu, l)}.$$

When ν takes $1, 2, \dots$, we get a sequence of infinite linear $[n_\nu, k_\nu]$ codes $\{C_{(\nu, l)}\}_{\nu=1}^\infty$.

Wan [8] is the first to use the theory of geometry of classical groups over finite fields to study the generalized Hamming weights of the codes from varieties, he determined the generalized Hamming weights of the codes from nondegenerate quadrics and prove that the codes satisfies the chain condition. In [9] Wan and Wu determined the weight hierarchies an generalized weight spectra of the codes from degenerate quadrics by using the geometry orthogonal groups.

3 The weight hierarchies of the codes

We denote by $\mathbb{F}_q^{(k)}$ (resp. $PG(k-1, \mathbb{F}_q)$) the k dimensional vector space (resp. $(k-1)$ dimensional projective space) over \mathbb{F}_q . A q -ary linear $[n, k]$ code C is called a *projective code* if the columns of a generator matrix G of C can be regarded as distinct points of $PG(k-1, \mathbb{F}_q)$. So we have a point set in $PG(k-1, \mathbb{F}_q)$, whose

elements are the column vectors of G , which will be denoted by $\mathcal{S}_{C,G}$ and called the point set arising from C via G . Different encoding matrices of C give rise to point sets which are projectively equivalent.

Two projective $[n, k]$ codes over \mathbb{F}_q are said to be *equivalent*, if one can be obtained from the other by permuting the coordinates of the codewords and multiplying them by non-zero elements of \mathbb{F}_q .

Let G be a generator matrix of a projective $[n, k]$ code C and C' be a projective code equivalent to C . Then the same transformation which transforms C to C' will transform the encoding matrix G of C to an encoding matrix G' of C' . If G and G' are encoding matrices of two equivalent projective $[n, k]$ codes C and C' , then $\mathcal{S}_{C,G}$ and $\mathcal{S}_{C',G'}$ are projectively equivalent.

Let G be a generator matrix of C , and for any column vector $x \in \mathbb{F}_q^{(k)}$, let $m_G(x)$ be the number of occurrences of the vector x as columns of G . Obviously, $w_s(C) = n - m_G(0^{(k)})$, where $0^{(k)}$ is the zero vector of $\mathbb{F}_q^{(k)}$. Let U be a subspace of $\mathbb{F}_q^{(k)}$ and define

$$m_G(U) = \sum_{x \in U} m_G(x).$$

If M is an $r \times k$ matrix of rank r , then MG generates a r -dimensional subcode of C , and any r -dimensional subcode is obtained in this way. Let D be an r -dimensional subcode of C and MG be a generator matrix of D , where M is an $r \times k$ matrix of rank r . Define the *dual* of D to be

$$D^\perp = \{x \in \mathbb{F}_q^{(k)} \mid Mx = 0\}, \quad (1)$$

Then D^\perp is an $(k - r)$ -dimensional subspace. From linear algebra we have

Lemma 1 ([12]): *For any r , where $1 \leq r \leq k$, the map $D \mapsto D^\perp$ defined by (1) is a bijection from the set of r -dimensional subcodes of C to the set of $(k - r)$ -dimensional subspaces of $\mathbb{F}_q^{(k)}$. \square*

Lemma 2 ([12]): *Let D be a subcode of C . Then*

$$w_s(D) = n - m_G(D^\perp).$$

Proof: Let MG be a generator matrix of D . Then $w_s(D) = n - m_{MG}(0^{(k)}) = n - \sum_{x \in D^\perp} m_G(x) = n - m_G(D^\perp)$. \square

Lemma 3 ([12]): *Let C be a q -ary projective $[n, k]$ code, G be a generator matrix of C , and $\mathcal{S}_{C,G}$ be the point set in $PG(k - 1, \mathbb{F}_q)$ arising from C via G . For any r , where $1 \leq r \leq k$, let D_r be an r -dimensional subcode, then there is an $(k - r - 1)$ -flat of $PG(k - 1, \mathbb{F}_q)$, P_{k-r-1} , such that*

$$w_s(D_r) = n - |P_{k-r-1} \cap \mathcal{S}_{C,G}|,$$

and

$$d_r(C) = n - \max\{|P_{k-r-1} \cap \mathcal{S}_{C,G}|\},$$

where P_{k-r-1} runs through all $(k-r-1)$ -flats of $PG(k-1, \mathbb{F}_q)$.

Proof: It follows from Lemmas 1, and 2. Specializing Lemma of [13] to any q -ary projective $[n, k]$ code C we can also obtain the second assert of the theorem. \square

4 The chain condition of the codes from Hermitian varieties

Let P be an m -dimensional vector subspace of $\mathbb{F}_{q^2}^{(k)}$, then there is a $m \times k$ matrix, such that its row vectors is a basis of P , we call the matrix a matrix representation of P . An m -dimensional vector subspace of $\mathbb{F}_{q^2}^{(k)}$ is also called a (projective) $(m-1)$ -flat of $PG(k-1, \mathbb{F}_{q^2})$. If no ambiguity arises, we denote all of them by P .

Two $n \times n$ matrices A and B over \mathbb{F}_{q^2} are said to be *cogredient*, if there is an $n \times n$ nonsingular matrix Q such that $QA {}^t\overline{A} = B$. Let P be an m -dimensional subspace of $\mathbb{F}_{q^2}^{(k)}$. P and its corresponding $(m-1)$ -flat are said to be *type* (m, s) if ${}^tPI_{(\nu, l)}\overline{P}$ is cogredient to

$$\begin{pmatrix} I^{(s)} & \\ & 0^{(m-s)} \end{pmatrix},$$

where $I^{(s)}$ is the $s \times s$ unit matrix, and $0^{(m-s)}$ is the $(m-s) \times (m-s)$ matrix whose entries are all 0. Let E be the subspace of $\mathbb{F}_{q^2}^{(\nu+l)}$ generated by $e_{\nu+1}, \dots, e_{\nu+l}$, where e_i is the length $\nu+l$ vector, whose i -th position is 1, and other positions are all 0. An m -dimensional subspace P or an $(m-1)$ -flat P is said to be *type* (m, s, t) if

- (1) P is of type (m, s) and
- (2) $\dim(P \cap E) = t$.

The following results will be used in the sequel and can be found in [14].

Lemma 4 In $PG(k-1, \mathbb{F}_{q^2})$, there exist flats of type (m, s, t) if and only if

$$t \leq l \quad \text{and} \quad 2s \leq 2(m-t) \leq \nu + s. \quad (3)$$

\square

Lemma 5 In $PG(k-1, \mathbb{F}_{q^2})$, there exist flats of type (m, s) if and only if

$$\max\{0, \frac{2m - \nu - s}{2}\} \leq \min\{l, m - s\}. \quad (4)$$

\square

Lemma 6 Let $m \geq 1$ and P be an $(m-1)$ -flat of type (m, s, t) or of type (m, s) . Then

$$|P \cap I_{(\nu, l)}| = \frac{q^{2m-1} + (-1)^s q^{2m-s} + (-1)^{s-1} q^{2m-s-1} - 1}{q^2 - 1}.$$

□

The generalized Hamming weights of $C_{(\nu, l)}$ are determined in [12].

Theorem 1 ([12]): The generalized Hamming weights of the q^2 -ary projective $[n, k]$ code $C_{(\nu, l)}$ is as follows.

1) When ν is even,

$$d_r(C_{(\nu, l)}) = \begin{cases} \frac{q^{2\nu+2l-1} - q^{2(\nu+l-r)-1}}{q^2 - 1}, & \text{for } r = 1, 2, \dots, \nu/2, \\ \frac{q^{2\nu+l-1} - q^{\nu+2l-1} + q^{\nu+2l} - q^{2(\nu+l-r)}}{q^2 - 1}, & \text{for } r = \nu/2, \dots, \nu + l. \end{cases}$$

2) When ν is odd,

$$d_r(C_{(\nu, l)}) = \begin{cases} \frac{q^{2\nu+2l-1} - q^{\nu+2l} - q^{2(\nu+l-r)-1} + q^{\nu+2l-2}}{q^2 - 1}, & \text{for } r = 1, \dots, (\nu-1)/2, \\ \frac{q^{2\nu+l-1} - q^{\nu+2l-1} + q^{\nu+2l} - q^{2(\nu+l-r)}}{q^2 - 1}, & \text{for } r = (\nu+1)/2, \dots, \nu + l. \end{cases}$$

□

Corollary 1 ([12]): Let ν be even and $r \leq \nu$. Then $d_r(C_{(\nu, l)})$ meets the Griesmer-Wei bound. □

Corollary 2 The sequence of infinite linear codes $\{C_{(\nu, l)}\}_{\nu=1}^{\infty}$ has a nonzero asymptotically relative minimum distance.

Proof: Consider $l = 0$. Let n_ν and d_ν be the code length and minimum distance of C_ν respectively, we have

$$n_\nu = \frac{q^{2\nu-1} - q^{\nu-1} + q^\nu - 1}{q^2 - 1}, \quad \text{and} \quad d_\nu = q^{2\nu-3},$$

so,

$$\delta_\nu = \frac{d_\nu}{n_\nu} \longrightarrow \frac{q^2 - 1}{q^2} > 0, (\nu \longrightarrow \infty).$$

□

Theorem 2 For any ν and l , codes $C_{(\nu, l)}$ satisfy the chain condition.

Proof: Let P be an $(m-1)$ -flat of type (m, s, t) , where $m = k - r = \nu + l - r$. Then

$$|P \cap I_{(\nu, l)}| = \frac{q^{2m-1} + (-1)^s q^{2m-s} + (-1)^{s-1} q^{2m-s-1} - 1}{q^2 - 1} = \frac{q^{2(\nu+l-r)-1} - 1}{q^2 - 1} + \frac{q^{2(\nu+l-r)-1}}{q+1} \left(-\frac{1}{q}\right)^s.$$

In $PG(k-1, \mathbb{F}_{q^2})$, there exist $(m-1)$ -flats of type (m, s, t) if and only if

$$2s \leq 2(m-t) \leq \nu + s,$$

as $m = \nu + l - r$,

$$2s \leq 2(\nu + l - r - t) \leq \nu + s. \quad (5)$$

If ν is even. We consider the following two cases.

(1) When $2r \leq \nu$, i.e., $r = 1, 2, \dots, \frac{\nu}{2}$, from (5), we have

$$s \geq \nu - 2r + 2(l - t).$$

Let $t = l$, (5) becomes $\nu - 2r \leq s \leq \nu - r$, so when P_{k-r-1} runs through all $(k-r-1)$ -flats, $\max\{|P_{k-r-1} \cap I_{(\nu, l)}|\}$ is achieved by $(\nu + l - r - 1)$ -flats of type $(\nu + l - r, \nu - 2r, l)$. Let $P_{\nu+l-2}$ be an $(\nu + l - 2)$ -flat of type $(\nu + l - 1, \nu - 2, l)$, then

$$d_1(C_{(\nu, l)}) = n - |P_{\nu+l-2} \cap I_{(\nu, l)}|.$$

Let $P_{\nu+l-3}$ be an $(\nu + l - 3)$ -flat of type $(\nu + l - 2, \nu - 4, l)$, then

$$d_2(C_{(\nu, l)}) = n - |P_{\nu+l-3} \cap I_{(\nu, l)}|.$$

And obviously we can assume that $P_{\nu+l-3} \subset P_{\nu+l-2}$. Proceeding in this way, we find a chain of flats $P_{\nu+l-4}$ of type $(\nu + l - 4, \nu - 6, l)$, \dots , $P_{\nu+l-i-1}$ of type $(\nu + l - i, \nu - 2i, l)$, $i = 3, 4, \dots, \frac{\nu}{2}$, with

$$d_i(C_{(\nu, l)}) = n - |P_{\nu+l-i-1} \cap I_{(\nu, l)}|,$$

and $P_{\frac{\nu}{2}+l-1} \subset P_{\frac{\nu}{2}+l} \subset \dots \subset P_{\nu+l-3} \subset P_{\nu+l-2}$.

(2) When $2r > \nu$, i.e., $r = \frac{\nu}{2} + 1, \dots, \nu + l$, when $\frac{\nu}{2} + l - r \leq t \leq \nu + l - r$, we can take $s = 0$, and when P_{k-r-1} runs through all $(k-r-1)$ -flats, $\max\{|P_{k-r-1} \cap I_{(\nu, l)}|\}$ is achieved by $(k-r-1)$ -flats of type $(\nu + l - r, 0, t)$. Let $P_{\frac{\nu}{2}+l-2}$ be an $(\frac{\nu}{2} + l - 1, 0, t)$ flat, where $l - 1 \leq t \leq \frac{\nu}{2} + l - 1$, then

$$d_{\frac{\nu}{2}+1}(C_{(\nu, l)}) = n - |P_{\frac{\nu}{2}+l-2} \cap I_{(\nu, l)}|.$$

And obviously we can assume $P_{\frac{\nu}{2}+l-2} \subset P_{\frac{\nu}{2}+l-1}$. Proceeding in this way, we can find a chain of flats

$$P_{-1} \subset P_0 \subset \dots \subset P_{\frac{\nu}{2}+l-2} \subset P_{\frac{\nu}{2}+l-1}.$$

Combine (1) and (2), we get a chain of flats

$$P_{-1} \subset P_0 \subset \dots \subset P_{\frac{\nu}{2}+l-2} \subset P_{\frac{\nu}{2}+l-1} \subset \dots \subset P_{\nu+l-2},$$

where $P_{\nu+l-i-1}$ is a $(\nu+l-i-1)$ -flat of type $(\nu+l-i, \nu-2i, l)$, when $i = 1, 2, \dots, \frac{\nu}{2}$; $P_{\nu+l-i-1}$ is a $(\nu+l-i-1)$ -flat of type $(\nu+l-i, 0, t)$, where $\frac{\nu}{2} + l - i \leq t \leq \nu + l - i$, when $i = \frac{\nu}{2} + 1, \dots, \nu + l - 1$, respectively, and $P_{-1} = 0$, such that

$$d_i(C_{(\nu,l)}) = n - |P_{\nu+l-i-1} \cap I_{(\nu,l)}|,$$

for $i = 1, 2, \dots, \nu + l$. Let

$$M_i = P_{\nu+l-i-1}^\perp = \{(x_1, \dots, x_k) \in \mathbb{F}_{q^2}^{(k)} \mid \begin{matrix} (x_1, \dots, x_k)^t (y_1, \dots, y_k) = 0, \\ \forall (y_1, \dots, y_k) \in P_{\nu+l-i-1} \end{matrix} \}.$$

Then M_i is an i -dimensional subspace of $\mathbb{F}_{q^2}^{(k)}$, and

$$M_1 \subset M_2 \subset \dots \subset M_{\nu+l} = \mathbb{F}_{q^2}^{(k)}.$$

Denote also by M_i a matrix representation of the i -dimensional subspace M_i of $\mathbb{F}_{q^2}^{(k)}$, and let

$$D_i = M_i G,$$

where G is the generator matrix of code $C_{(\nu,l)}$. Then D_i is an i -dimensional subcode of $C_{(\nu,l)}$ and by lemmas 2 and 3,

$$w_s(D_i) = n - |P_{\nu+l-i-1} \cap I_{(\nu,l)}|.$$

So we have a chain of subcodes

$$D_1 \subset D_2 \subset \dots \subset D_{\nu+l} = C_{(\nu,l)},$$

such that

$$w_s(D_i) = d_i(C_{(\nu,l)}),$$

for $i = 1, 2, \dots, \nu + l$. So when ν is even, $C_{(\nu,l)}$ satisfies the chain condition. If ν is odd, the proof is similar, we omit the details. \square

Theorem 3 *For any ν and l , the dual codes $C_{(\nu,l)}^\perp$ satisfy the chain condition.*

Proof: It is a corollary of Theorem 2 and Theorem 5 of [11]. \square

5 Conclusions

It is a challenging problem to determine the complete weight hierarchies of linear codes. Even for some classical codes, such as BCH codes, generalized Reed-Muller codes, etc., this problem is still unsolved. The chain condition is very useful in the study of weight hierarchies of product codes. We have proved that the codes from Hermitian varieties and their dual codes satisfy the chain condition. It is very interesting to study the weight hierarchies of some product codes by the codes from Hermitian varieties or their dual codes and other linear codes.

References

- [1] V. K. Wei, Generalized Hamming weights for linear codes, *IEEE Trans. Inform. Theory* **IT-37** (1991), 1412-1418.
- [2] B. Chor, O. Goldreich, J. Hastad, J. Friedmann, S. Rudish, R. , The bit extraction problem of t -resilient functions, *Proc. 20th Symp. Foundation Comput. Sci.*, (1985), 396-407.
- [3] J. K. Wolf, Efficient Maximum Likelihood Decoding of Linear Block Codes Using a Trellis, *IEEE Trans. Inform. Theory* **IT-24**, (1978), 76-78.
- [4] T. Kasami, T. Takata, T. Fujiwara, Shu Lin, On the Optimum Bit Orders with Respect to the State Complexity of Trellis Diagrams for Binary Linear Codes, *IEEE Trans. Inform. Theory* **IT-39**, (1993), 242-245.
- [5] T. Helleseth, P. V. Kumar, The weight hierarchy of the Kasami codes, preprint.
- [6] G. L. Feng, K. K. Tzeng, V. K. Wei, On the generalized Hamming weights of several classes of cyclic codes, *IEEE Trans. Inform. Theory* **IT-38** (1992), 1125-1130.
- [7] J. W. P. Hirschfeld, M. A. Tsfasman, S. G. Vladut, The weight hierarchy of higher-dimensional Hermitian codes, *IEEE Trans. Inform. Theory* **IT-40** (1994), 275-278.
- [8] Z. Wan, The weight hierarchies of the projective codes from nondegenerate Quadrics, *Designs, Codes and Cryptography*, **4**, 1994, 283-300.
- [9] Z. Wan and Xinwen Wu, The weight hierarchies and generalized weight spectra of the projective codes from degenerate quadrics, to appear in *Discrete Mathematics*.
- [10] T. Helleseth, T. Kløve, J. Mykkeltveit, The weight distribution of irreducible cyclic codes with block length $n_1(\frac{(q^l-1)}{N})$, *Discrete Mathematics*, **18**(1977), 179-211.
- [11] V. K. Wei and K. Yang, On the generalized Hamming weights of squaring construction and product codes, *IEEE Trans. Inform. Theory* **IT-39** (1993), 1709-1713.
- [12] Xinwen Wu, Generalized Hamming weights of some classes of projective codes, Ph.D. Dissertation, Institute of Systems Science, Chinese Academy of Sciences, 1995.

- [13] T. Helleseeth, T. Kløve, Φ . Ytrehus, Generalized Hamming Weights of Linear Codes, *IEEE Trans. Inform. Theory*, **38**(1992), 1133-1140.
- [14] Z. Wan, Geometry of Classical Groups over Finite Fields, Studentlitteratur, Lund, 1993.